International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC)
ISSN (P): 2250-1568; ISSN (E): 2278-9448
Vol. 9, Issue 1, Jun 2019, 1-4

ENHANCED IDENTITY-BASED SIGNCRYPTION SYSTEM

V. ISAKKIRAJAN[1] & M. RAMAKRISHNAN[2]

[1]*Research Scholar, Manonmaniam Sundaranar University, Tirunelveli, Tamil Nadu, India*

[2]*Department of Computer Applications, Madurai Kamaraj University, Madurai, Tamil Nadu, India*

ABSTRACT

A combination of encryption and signature is a cryptosystem called traditional signcryption, wherein sender authentication is considered a key task to be verified by third party or judge. Without the knowledge of the sender, the judge can authenticate the message using the receiver decryption parameters and the process is called the signcryption scheme.

The paper's objective is to analyse the security and confidentiality of message and then to integrate authentication, enforceability, forward secrecy, public verifiable along with packet mechanisms. In this study, using the SSL mechanism the information to be sent is split into various parts and are all parts collected at the receiver end. This mechanism proved to be resource efficient, producing high precise results compared to the previous one.

KEYWORDS: Signcryption, Identity, Cryptography & Authentication

Received: Dec 19, 2018; **Accepted:** Jan 09, 2019; **Published:** Jan 22, 2019; **Paper Id.:** IJCNWMCJUN20191

Original Article

INTRODUCTION

The basic cryptographic tools are digital signature and encryption, ensuring confidentiality, integrity, and non-repudiation, which were seen as the distinct building blocks of various cryptographic systems. The traditional method involved a message of a digital sign which is the encrypted (signature-then-encryption). The following are the two problems of this traditional method: Low efficiency and high cost of such summation and that any arbitrary schemes cannot guarantee security. The recent method is signcryption which comprises digital signature and encryption in a single logical step, thereby effectively decreasing the computational costs and communication overheads in comparison with the traditional signature-then-encryption method.

The efficiency of the signcryption method, that is, providing both digital signatures and encryption simultaneously is better than the traditional digital signature and encryption schemes..

The computational costs, communication overheads, correctness, and efficiency are the merits of the signcryption scheme. Other features of signcryption include the following: Confidentiality, Unforgeability, Integrity, and Non-repudiation and also Public verifiability and Forward secrecy of message confidentiality.

The encryption schemes are currently based on bilinear pairings on elliptic curves, such as the Weil or Tate pairings. The first schemes was developed by Dan Boneh and Matthew K. Franklin (2001), whose approach is based on probabilistic encryption of arbitrary cipher texts using Elgamal-like aspect. In many elliptic curve groups, the Boneh-Franklin scheme is considered secure, but the security proof rests on relatively new assumptions about the hardness of problems.

In 2001, Clifford Cocks proposed another identity-based encryption called Cocks IBE scheme. The base of this scheme involves well-studied assumptions (the quadratic residuosity assumption) which encrypts one bit message at a time but with a high degree of cipher text expansion.

For transmission the private key, it is a must to have a secure channel between a user and the Private Key Generator (PKG), which should be achieved on joining the system. For a large-scale system, an SSL-like connection is a right solution. It has be remembered that PKG users must be able to authenticate themselves, which can be done using username, password or through public key pairs managed on smart cards.

Implementation of Identity-Based Signcryption

Key Generation (Gen), Signcryption (SC), and Unsigncryption (USC) are the three algorithms of signcryption scheme. Gen generates a pair of keys for any user, SC is generally a probabilistic algorithm, and USC is the most likely deterministic.

Extended Euclidian Method

```
public BigInteger extendedEuclid(BigInteger a, BigIntegerb) {

    BigInteger x = BigInteger.valueOf(1);
    y = BigInteger.valueOf(0);

    BigInteger xLast = BigInteger.valueOf(0);
    yLast = BigInteger.valueOf(0);

    BigIntegerq, r, m, n;

    while(a.compareTo(BigInteger.valueOf(0)) != 0) {

    q = b.divide(a);
    r = b.remainder(a);

    m = xLast.subtract(q.multiply(x));

    n = yLast.subtract(q.multiply(y));

    xLast = x;
    yLast = y;

    x = m;
    y = n;
    b = a;
    a = r;

    }

    if(xLast.compareTo(BigInteger.valueOf(0))<0)
        xLast =
xLast.add((this.p.subtract(BigInteger.ONE)).multiply(this.q.subtract(BigInteger.ONE)));
returnxLast;

}
```

A complete identity-based encryption system consists of four algorithms.

- **Setup:** The whole IBE environment is created by this algorithm run by PKG. Here the master key is kept secret, which is also used to derive the users' private keys, while the system parameters are made public. It accepts a security parameter {\displaystyle \textstyle k}k and outputs:
  - A set {\displaystyle \textstyle {\mathcal {P}}}P of system parameters including the message space and cipher text space {\displaystyle \textstyle {\mathcal {M}}}M and {\displaystyle \textstyle {\mathcal {C}}} C
  - A master key {\displaystyle \textstyle K_{m}} Km.
- **Extract:** When a user requests his/her private key, this algorithm is used and is run by PKG. The IBE protocols considers the following as its problem: the verification of the authenticity of the requestor and the secure transport of {\displaystyle \textstyle d}d and hence ignores them. It takes as input {\displaystyle \textstyle {\mathcal {P}}}P,Km {\displaystyle \textstyle K_{m}} and an identifier {\displaystyle \textstyle ID\in \left\{0,1\right\}^{*}} ID€{0,1} and returns the private key {\displaystyle \textstyle d}d for user {\displaystyle \textstyle ID}ID.
- **Encrypt:** Takes {\displaystyle \textstyle {\mathcal {P}}}P, a message {\displaystyle \textstyle m\in {\mathcal {M}}}m€M and {\displaystyle \textstyle ID\in \left\{0,1\right\}^{*}} ID€{0,1} and outputs the encryption {\displaystyle \textstyle c\in {\mathcal {C}}}c€C
- **Decrypt:** Accepts {\displaystyle \textstyle d}d, P{\displaystyle \textstyle {\mathcal {P}}} and {\displaystyle \textstyle c\in {\mathcal {C}}}c€C and returns {\displaystyle \textstyle m\in {\mathcal {M}}}m€M

ASCII string is a known identity value that can be used to generate the identity of a public key. The PKG uses the master private key to generate the private key for identity ID.

CONCLUSIONS

Authentic messages can be delivered between senders and receivers using the identity-based signcryption scheme.

To precisely implement all facets of the aforementioned identity-based signcryption, this study presents a new cryptographic scheme whose mechanism is based on SSL.

REFERENCES

1. *N. Koblitz and A. Menezes, "Intractable problems in cryptography," in Proceedings of the 9th International Conference on Finite Field and Their Applications, Contemporary Mathematics, pp.279–300, 2010.*
2. *D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures," Journal of Cryptology, vol. 13, no. 3, pp. 361–396, 2000.*
3. *Y. F. Chung, K. H. Huang, F. Lai, and T. S. Chen, "ID-based digital signature scheme on the elliptic curve cryptosystem," Computer Standards & Interfaces, vol. 29, no. 6, pp. 601–604, 2007.*
4. *S. K. H. Islam and G. P. Biswas, "A pairing-free identity-based authenticated group key agreement protocol for imbalanced mobile networks," Annals of Telecommunications-Annales des T´el´ecommunications, vol. 67, no. 11-12, pp. 547–558, 2012.*
5. *S. K. H. Islam and G. P. Biswas, "Provably secure and pairingfree certificateless digital signature scheme using elliptic curve*

cryptography," International Journal of Computer Mathematics, vol. 90, no. 11, pp. 2244–2258, 2013.

6. *Sattam S. Al-Riyami and Kenneth G. Paterson, Certificateless Public Key Cryptography, Lecture Notes in Computer Science, pp. 452 – 473, 2003*
7. *D. Galindo. Boneh-Franklin Identity Based Encryption Revisited. In ICALP 05, LNCS 3580, pages 791–802.*
8. *Jianhong Zhang, Zhipeng Chen, Min Xu "On the Security of ID-based Multi-receiver Threshold Signcryption Scheme", In proceedings of 2nd International Conference on Consumer Electronics, Communications and Networks (CECNet), pp. 1944 – 1948, 2012.*
9. *Baek J, Steinfeld R, Zheng Y. Formal proofs for the security of signcryption. Journal of Cryptology. 2007;20(2):203–235*
10. *Calderbank, Michael The RSA Cryptosystem: History, Algorithm, Primes 2007-08-20*
11. *Moon, T. K. (2005). Error Correction Coding: Mathematical Methods and Algorithms. John Wiley and Sons. p. 266*